Web Hacking Black Belt Edition

Learn via: **Classroom / Virtual Classroom / Online**

Duration: **5 Day**

https://bilginc.com/en/training/web-hacking-black-belt-edition-690-training/

Overview

This class teaches the audience a wealth of hacking techniques to compromise modern-day web applications, APIs and associated end-points. This class focuses on specific areas of appsec and on advanced vulnerability identification and exploitation techniques. The class allows attendees to learn and practice some neat, new and ridiculous hacks which affected real-life products and have found a mention in real bug-bounty programs. The vulnerabilities selected for the class either typically go undetected by modern scanners or the exploitation techniques are not so well known.

Attendees will also benefit from a state-of-art Hacklab during the course.

Some of the highlights of the class include:

- Modern JWT, SAML, OAuth bugs
- Core business logic issues
- Practical cryptographic flaws.
- RCE via Serialization, Object, OGNL and template injection.
- Exploitation over DNS channels
- Advanced SSRF, HPP, XXE and SQLi topics.
- Serverless exploits
- Web Caching issues
- Attack chaining and real life examples.

Target Audience

- Web developers
- Intermediate level penetration testers
- DevOps engineers, network engineers
- Security researchers / analysts
- Security architects
- Security professionals & enthusiasts
- Anyone who wants to take their skills to the next level

Users are also encouraged to familiarize themselves with Burp Suite https://portswigger.net/burp/communitydownload to gain maximum out of the class.

What You Will Learn

Harden your perimeter, lower the risk of compromise, and make your organisation a less attractive target for attackers by building a team that can identify, test, and guide developers to secure web-based vulnerabilities.

Trained delegates can:

- Perform security testing to identify and safely exploit complex web vulnerabilities that get missed by scanners and other automated tools – this can help you detect vulnerabilities and recommend patching accordingly
- Design this testing around real-world attacker behaviour and tooling, making it relevant to the threats facing your organisation
- Customise offensive tooling to generate tailored (rather than "out of the box") payloads that lead to more advanced testing
- Recommend measures to circumvent any conditions that could lead to the emergence of vulnerabilities
- Understand the business impact of web vulnerabilities and articulate this to key stakeholders
- Take on greater responsibility in the team and become an advocate of security in the wider business

Outline

The latest hacks in the world of web hacking. The class content has been carefully handpicked to focus on some neat, new and ridiculous attacks. We provide a custom kali image for this class. The custom kali image has been loaded with a number of plugins and tools (some public and some

NotSoPublic) and these aid in quickly identifying and exploiting vulnerabilities discussed during the class.

The class is taught by a real pen tester and the real-world stories shared during the class help attendees in putting things into perspective. Access to a hacking lab during the course and numerous scripts and tools will also be provided during the training, along with student handouts. Our courses also come with detailed answer sheets. That is a step by step walkthrough of how every exercise within the class needs to be solved. These answer sheets are also provided to students at the end of the class.

Lab Setup and architecture overview

Introduction to Burp Features

Attacking Authentication and SSO

- Token Hijacking attacks
- Logical Bypass / Boundary Conditions
- Bypassing 2 Factor Authentication
- Authentication Bypass using Subdomain Takeover
- JWT/JWS Token attacks
- SAML Authorization Bypass
- OAuth Issues

Password Reset Attacks

- Session Poisoning
- Host Header Validation Bypass
- Case study of popular password reset fails

Business Logic Flaws / Authorization flaws

- Mass Assignment
- Invite/Promo Code Bypass
- Replay Attack
- API Authorisation Bypass
- HTTP Parameter Pollution (HPP)

XML External Entity (XXE) Attack

- XXE Basics
- Advanced XXE Exploitation over OOB channels
- XXE through SAML
- XXE in File Parsing

Breaking Crypto

- Known Plaintext Attack (Faulty Password Reset)
- Padding Oracle Attack
- Hash length extension attacks
- Auth bypass using .NET Machine Key
- Exploiting padding oracles with fixed IVs

Remote Code Execution (RCE)

- Java Serialization Attack
- .Net Serialization Attack
- PHP Serialization Attack
- Python serialization attack
- Server Side Template Injection
- Exploiting code injection over OOB channel

SQL Injection Masterclass

- 2nd order injection
- Out-of-Band exploitation
- SQLi through crypto
- OS code exec via PowerShell
- Advanced topics in SQli
- Advanced SQLMap Usage and WAF bypass
- Pentesting GraphQL

Tricky File Upload

- Malicious File Extensions
- Circumventing File validation checks
- Exploiting hardened web servers
- SQL injection via File Metadata

Server-Side Request Forgery (SSRF)

- SSRF to query internal network
- SSRF to exploit templates and extensions
- SSRF filter bypass techniques
- Various Case studies

Attacking the Cloud

- SSRF Exploitation
- Serverless exploitation
- Google Dorking in the Cloud Era
- Cognito misconfiguration to data exfiltration
- Post Exploitation techniques on Cloud-hosted applications
- Various Case Studies

Attacking Hardened CMS

- Identifying and attacking various CMS
- Attacking Hardened Wordpress, Joomla, and Sharepoint

Web Caching Attacks

Miscellaneous Vulnerabilities

- Unicode Normalization attacks
- Second order IDOR attack
- Exploiting misconfigured code control systems
- HTTP Desync attack

Attack Chaining N tier vulnerability Chaining leading to RCE

Various Case Studies

- A Collection of weird and wonderful XSS and CSRF attacks

B33r-101